Universidad San Gregorio de Portoviejo Carrera de Derecho

Trabajo de Investigación de Artículo Científico previo a la obtención del título de Abogado

Título:

El derecho a la privacidad en la era de la realidad cibernética: retos de ciberseguridad

Autor:

Kevin Dayan Mero Demera

Tutor:

Dr. Javier Antonio Artiles Santana, PhD.

Portoviejo – Manabí - Ecuador

Octubre 2024 – marzo 2025

Declaración de autoría y cesión de derechos de propiedad intelectual

Yo, KEVIN DAYAN MERO DEMERA, con cédula de ciudadanía Nº 1314710904, declaro en forma libre y voluntaria, ser el autor del trabajo de investigación con el título "El derecho a la privacidad en la era de la realidad cibernética: retos de ciberseguridad" cuyo contenido es auténtico, original y no infringe derechos de propiedad intelectual de terceros. En este sentido, asumo la responsabilidad correspondiente ante cualquier falsedad, ocultamiento u omisión de la información obtenida en el proceso de investigación. Así como también los contenidos, ideas, análisis, conclusiones y propuestas son exclusiva responsabilidad de mi persona como autora.

De esta manera expresa, cedo los derechos de propiedad intelectual del Artículo Científico denominado: "El derecho a la privacidad en la era de la realidad cibernética: retos de ciberseguridad" a la Universidad San Gregorio de Portoviejo**,** por ser la institución de Educación Superior que me acogió en todo el proceso de desarrollo del mismo, y autorizo a su difusión en formato digital, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior

En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Universidad San Gregorio de Portoviejo.

Portoviejo, 11 de abril de 2025

Kevin Dayan Mero Demera

1314710904

El derecho a la privacidad en la era de la realidad cibernética: retos de ciberseguridad

The right to privacy in the era of cyber reality: cybersecurity challenges

Autor:

Kevin Dayan Mero Demera

Universidad San Gregorio de Portoviejo

ORCID: 0000-0001-9791-9379

Kdmd1314710904@gmail.com

Tutor:

Dr. Javier Antonio Artiles Santana, PhD.

Universidad San Gregorio de Portoviejo

ORCID: 0000-0001-8897-7710

jaartiles@sangregorio.edu.ec

Resumen

En el marco del desarrollo tecnológico actual en la que las tecnologías emergentes basadas en el análisis de datos han desarrollado un nuevo espacio digital en el que confluye gran cantidad de información, se plantean nuevos retos relativos a la protección de derechos especialmente aquellos relacionados con la privacidad y la información. En este sentido, a fin de plantear alternativas que respondan a dicha necesidad, el objetivo de esta investigación es analizar el impacto del desarrollo de nuevas tecnologías en el derecho a la privacidad desde la perspectiva de la ciberseguridad, empleando para el efecto un enfoque de investigación cualitativo de carácter descriptivo basado en la revisión bibliográfica y el análisis de contenido. Los resultados de la investigación determinan que existe un considerable incremento de vulnerabilidades en la privacidad, lo que plantea nuevos desafíos regulatorios con la necesidad de una legislación dinámica y adaptable para con las nuevas tecnologías, por lo que frente a la creciente tensión entre la tecnológica y los derechos fundamentales, la ciberseguridad tiene un rol protagónico en la protección de la privacidad y otros derechos conexos. Por lo expuesto, se concluye que es imprescindible que se adopte un enfoque

multidimensional en la era digital capaz de combinar regulaciones dinámicas, estrategias de ciberseguridad y principios éticos como la autonomía y la justicia en el desarrollo tecnológico.

Palabras clave: Ciberseguridad; derechos fundamentales; información; privacidad; tecnologías

Abstract

Within the framework of current technological development, in which emerging technologies based on data analysis have developed a new digital space where vast amounts of information converge, new challenges arise regarding the protection of rights, especially those related to privacy and information. In this sense, in order to propose alternatives that respond to this need, the objective of this research is to analyze the impact of the development of new technologies on the right to privacy from the perspective of cybersecurity, employing a descriptive qualitative research approach based on bibliographic review and content analysis. The results of the research determine a considerable increase in privacy vulnerabilities, which poses new regulatory challenges with the need for dynamic and adaptable legislation for new technologies. Therefore, in the face of the growing tension between technology and fundamental rights, cybersecurity has a leading role in the protection of privacy and other related rights. Based on the above, we conclude that it is essential to adopt a multidimensional approach in the digital age, capable of combining dynamic regulations, cybersecurity strategies, and ethical principles such as autonomy and fairness in technological development.

Keywords: Cybersecurity; fundamental rights; information; privacy; technologies

Introducción

En el contexto socio jurídico actual el derecho a la privacidad se encuentra inmerso en una serie de desafíos por la transformación de las sociedades producto de las nuevas tecnologías que a decir de Rivera y Maldonado (2023), revolucionan por completo la forma de vivir por cuanto transforman los datos en información para tomar decisiones incluso sin partir de

principios legales como el consentimiento informado o la seguridad de la información.

El uso de tecnologías emergentes, como la inteligencia artificial y el Internet amplía el espectro de vulnerabilidades que requieren de una revisión y actualización constante de las políticas y leyes que atiendan a la protección y mantenimiento de los derechos y bienes jurídicos de las personas; por ende, esta situación demanda una acción inmediata y coordinada para asegurar que las normativas no solo sean reactivas, sino también proactivas, anticipando posibles riesgos y desarrollando estrategias efectivas de prevención y mitigación considerando que, tal y como lo menciona Fraguas (2024), la privacidad es un bien preciado y un desafío fundamental en la era digital actual que se encuentra constantemente expuesto por lo que Mendivelso (2024) llama información líquida ocasionada por la alta influencia de datos.

Ahora bien ¿cómo afecta el desarrollo de las nuevas tecnologías al derecho a la privacidad y qué medidas pueden implementarse desde la ciberseguridad para la protección de datos personales dentro del marco normativo vigente? Para resolver esta interrogante, se plantea como objetivo analizar el impacto del desarrollo de nuevas tecnologías en el derecho a la privacidad desde la perspectiva de la ciberseguridad, cuyas tareas científicas son: identificar los riesgos y desafíos para la privacidad derivados del uso de tecnologías emergentes, evaluar el rol de la ciberseguridad desde el punto de vista jurídico en la protección de la privacidad y diseñar prácticas y políticas que permitan equilibrar la innovación tecnológica con el respeto a los derechos de los usuarios

Esta investigación se encuentra justificada en el hecho de que la protección del derecho a la privacidad dentro de una sociedad tecnológica constituye un desafío socio jurídico de carácter global por cuanto a medida que las tecnologías avanzan, la privacidad enfrenta nuevas amenazas, como el uso indebido de datos personales, ciberataques y vigilancia masiva, lo que directamente pone en riesgo la dignidad humana debido a la vulnerabilidad de los derechos en el entorno digital.

Es por este motivo que se vuelve imprescindible la adopción de enfoques innovadores que

desde el punto de vista jurídico logren un equilibrio entre la innovación tecnológica y los derechos fundamentales, lo que consecuentemente se traduce en la protección efectiva de los ciudadanos. De esta manera, el estudio no o solo busca aportar al conocimiento teórico sobre la relación entre tecnología, privacidad y ciberseguridad, sino también ofrecer recomendaciones prácticas sobre marcos regulatorios eficaces y eficientes capaces de proteger el derecho a la privacidad.

Es decir, este estudio responde a la necesidad urgente de proteger la privacidad en un panorama tecnológico en constante cambio, armonizando el progreso con la salvaguarda de los derechos humanos por cuanto ciberseguridad ha llegado a convertirse en un elemento crítico para el funcionamiento adecuado y seguro de las sociedades modernas; en razón de esto, los sistemas jurídicos actuales toman un papel trascendental para crear y determinar preceptos legales que protejan los derechos y bienes jurídicos más importantes presentes en el mundo digital; en este sentido, el estudio busca destacar la importancia de diseñar marcos legales flexibles y dinámicos, que no sólo respondan a las amenazas actuales, sino que también anticipen las futuras, incorporando principios éticos y de derechos para garantizar una sociedad digital más segura y justa.

Metodología

El enfoque de investigación es cualitativo porque “se sitúa en un paradigma emergente de la ciencia, más interpretativo que cuantificador, que rechaza que la cuantificación positivista sea el modo apropiado para estudiar las problemáticas sociales y culturales” (Criado, 2021, p. 34). Es decir, en este estudio no se pretende sistematizar datos empíricos sino contextualizar la realidad jurídica actual en el marco de una sociedad que convive directamente con las nuevas tecnologías por cuanto el enfoque cualitativo da lugar a estudios enfocados en la realidad de los sujetos que se involucran en él.

En concordancia con aquello, el tipo de investigación jurídica seleccionado es el teórico, debido a que trabaja sobre dimensiones abstractas -en este caso, el derecho a la privacidad y la

ciberseguridad- que se estructuran de manera lógica con fundamentos dogmáticos para estructurar un marco de sentido en la construcción del estado del arte, por lo que se trata de unainvestigación jurídico-dogmática que, además, por su naturaleza abarca dimensiones históricas. (Criado, 2021).

Se trata, por lo tanto de un artículo de revisión en el que emplean los tres principales métodos de la doctrina investigativa jurídica, estos son: histórico, comparado y lógico (Martínez, 2023), que son los que establecen las directrices en el levantamiento de información cuya técnica principal es la revisión bibliográfica porque permite identificar las principales tendencias teórico-jurídicas respecto del tema objeto de estudio por cuanto para realizar la comprensión crítica del mismo es indispensable realizar un análisis exhaustivo de fuentes bibliográficas para el abordaje de teorías y argumentos; lo que se integra con el análisis de contenido cualitativo que según Ramírez (2021) es una herramienta complementaria que permite agrupar la discusión en torno a determinadas categorías temáticas.

Fundamentos teóricos

Internet, big data y vigilancia digital

El internet y los sistemas informáticos suponen un nuevo paradigma para el acceso a la información por cuanto logran que cada acción y movimiento se vea reflejada en la red o ciberespacio que hace referencia al escenario espacial que existía en el interior de las computadoras, sin embargo, en la actualidad este término es usado para definir el espacio antropológico de la red informática (Pons, 2017), lo que explica el vertiginoso aumento de los usuarios de internet que, de acuerdo con Agnese (2016), “en 1993 se estimaba que había 14 millones y en julio de 2015 rondaban los 2900 millones” (p. 4); lo que implica que el mundo se encuentra atravesando una verdadera revolución tecnológica que termina por volver difusas las líneas entre la realidad y el ciberespacio que, de acuerdo con Santana y Báez (2022) es un error semántico por cuanto el internet se limita a la existencia de hardware, software y códigos

específicos, mientras que el ciberespacio trasciende estos elementos a través de ordenadores y satélites.

Es decir, el ciberespacio está entrelazado con el internet, ya que a través de sus códigos y ordenadores llega a formar otro espacio donde los ciudadanos interactúan y comparten información, que en muchos casos esta información es relevante, ya que en ella también van sus datos personales que de acuerdo con Flores de Valgaz *et al.* (2024) hacen referencia a toda información que pertenecen a una persona para identificarla y se protegen en función de los derechos humanos y que se protegen de acuerdo a la gravedad y delicadeza de la información. Por cuanto, es la seguridad directamente aplicada a los datos y la información para la protección de los activos digitales (Vega *et al.*, 2024); que se complica por la existencia de un contexto mediático en el que convergen distintos tipos de comunicación e interacción social, que de la mano presentan un conjunto de riesgos relacionados con la prevalencia de los derechos (Miranda, 2023).

Es decir, pese a que la sociedad actual se encuentra globalmente digitalizada, la falta de recursos no solo incrementa la brecha digital, sino que disminuye la efectividad de las barreras de ciberseguridad que se pudieren implementar; ejemplo de esto, el caso de Ecuador donde a decir de Leyva (2021), “, la falta de decisión política y la limitación de recursos no permiten promover una conciencia plena de prevención y mitigación de los riesgos provenientes de la actividad ilícita con los medios digitales” (p. 1232).

Amenazas a la privacidad: recopilación de datos, perfilamiento y ciberataques

En contemporaneidad hablamos, entonces, de *ciber-problemas* que surgen y evolucionan al mismo tiempo de las nuevas tecnologías de la información y afectan más que solo los ordenadores por cuanto atacan los datos con herramientas de coerción directa con significativas ventajas relacionadas con el anonimato y la falta de estrategias de protección e identificación

(Quispe, 2024) especialmente de los datos personales que se encuentran constantemente expuestos a los delitos informáticos como el tráfico ilegal de datos o el *pishing* (Dávalos y Mujica, 2024).

Esto involucra la idea de ciberseguridad ante la especial exposición de los derechos en el contexto tecnológico pues, a decir de Candau (2021) existe una fuerte tendencia hacia los cibercrímenes que exigen que se desplieguen herramientas y servicios de ciberseguridad de alta disponibilidad. Es decir, resulta imprescindible que se robustezcan las medidas de ciberseguridad en el contexto actual de una sociedad que cada día convive más con las nuevas tecnologías y, por tanto, es tendiente a desarrollar nuevas conductas que pueden ser capaces de vulnerar derechos fundamentales relacionados con la privacidad, por ejemplo; por cuanto actualmente ya no solo se habla de redes de información y comunicación sino que incluso se involucra nuevos sistemas de inteligencia artificial que basan su funcionamiento en el aprendizaje automático cono fuertes incidencias en la seguridad individual (Beccerril, 2021).

En este contexto de dependencia generalizada de sistemas digitales, las ciber-amenazas pueden superar la capacidad de las sociedades para prevenir y gestionar de manera eficaz amenazas cibernéticas. Por ejemplo, la digitalización de las cadenas de suministro crea nuevas vulnerabilidades porque esas cadenas dependen de proveedores de tecnología y otros servicios de terceros, que también están expuestos a amenazas similares y potencialmente contagiosas. (Solleiro *et al.*, 2022, p. 10)

Se hace referencia, por tanto, al contraste entre el desarrollo tecnológico y el progreso socio jurídico para hacer frente a dichos cambios; de forma tal que se vuelve imperativo no solo el desarrollo de políticas sino también de planes y proyectos a corto plazo capaces de mitigar el impacto; de acuerdo con Giant (2016), la ciberseguridad constituye un conjunto de prácticas, tecnologías y procesos que se encuentran diseñados para proteger los sistemas, redes y datos ante

cualquier ataque cibernético, daños o accesos no autorizados, teniendo en cuenta, que su principal objetivo es garantizar la integridad, confidencialidad y disponibilidad de la información y los sistemas informáticos que de acuerdo con Gutiérrez *et al.* (2023), hacen frente a la responsabilidad social de integración responsable de las nuevas tecnologías.

Ciberseguridad como herramienta para la protección de la privacidad

Asimbaya (2024) lo concibe como un campo dinámico y esencial que deriva del progreso tecnológico global con la finalidad de brindar protección a infraestructuras críticas a nivel físico como virtual gracias al avance de las nuevas tecnologías y la propensión a ciberataques que afectan directamente a derechos relacionados con la seguridad digital de la información y los datos; motivo por el cual resulta por demás indispensable que el diseño de políticas públicas al respecto tome en consideración la dinámica democrática e institucional que trasciende el espacio físico y virtual con estrategias híbridas que logren hacer frente a la problemática para garantizar el uso legítimo de las nuevas tecnologías logrando un equilibrio con el Estado (Cano, 2022) por cuanto a decir de Plúas *et al.* (2024), es el pilar fundamental de protección de los derechos digitales y naturales por la incorporación de la tecnología en el ámbito legal a través del diseño y puesta en práctica de protocolos sólidos de seguridad.

En este orden de ideas, Montúfar (2022) resalta la existencia de políticas e instrumentos nacionales en Ecuador en relación a la ciberseguridad y ciberdefensa que se han aplicado, inicio en el 2013 con la creación del primer esquema gubernamental de seguridad de la información (EGSI) basado en la norma ISO 27001:2013, por la Secretaría Nacional de la Administración Pública (SNAP) que tenía como finalidad brindar seguridad en el uso de internet a los usuarios, inclusive también buscaba de implementar controles para garantizar la confidencialidad, integridad y disponibilidad de la información que se gestiona en las instituciones del Estado, por otro lado, para el año 2014 a partir del Acuerdo Ministerial 281 se crea el Sistema de

Ciberdefensa, en el cual se crea el Comando de Ciberdefensa (COCIBER), cabe recalcar, que ya para el año 2018 la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) crea una norma técnica para coordinar la gestión de incidentes y vulnerabilidades que afecten a la seguridad de las redes y servicios de telecomunicaciones.

En adición, la Ley de Comercio, Firmas electrónicas y Mensajes de datos en su artículo 5, establece La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos de Ecuador establece como principios fundamentales la confidencialidad y reserva para los mensajes de datos, independientemente de su forma, medio o propósito, teniendo por objeto garantizar la protección de la información, tanto personal como profesional, en el ámbito digital.

Este marco legal asegura que cualquier violación a estos principios, como la intrusión electrónica no autorizada, la transferencia ilegal de mensajes de datos, o la violación del secreto profesional, sea considerada una infracción grave y se sancione de acuerdo con lo estipulado en esta Ley y otras normas correspondientes; de tal manera, estableciendo sanciones claras para estas violaciones, la Ley no solo puede proteger la privacidad y seguridad de la información de los individuos y organizaciones, sino también fomentar la confianza en las transacciones y comunicaciones electrónicas, a través de un entorno digital seguro y confiable para el desarrollo económico y social del país.

En relación, la Ley Orgánica de Protección de datos en su artículo 40 determina que para analizar “riesgos, amenazas y vulnerabilidades, se deberá utilizar una metodología que considere, entre otras: 1) Las particularidades del tratamiento; 2) Las particularidades de las partes involucradas; y, 3) Las categorías y el volumen de datos personales objeto de tratamiento” (p.21).

No obstante, para dicho autor las normativas resultan insuficientes especialmente para determinados grupos prioritarios de atención como los niños, niñas y adolescentes, lo que para Florabel (2024), se torna en una situación alarmante por cuanto “la ausencia de mecanismos

legales hace que se incrementen los ataques y también la impunidad, porque no existen consecuencias jurídicas para los atacantes […] la regulación del ciberespacio le corresponde al DI pero pasa por la voluntad política de los Estados" (p. 179). De ahí que para Rodríguez *et al.* (2023), resulte imprescindible su abordaje desde el Derecho Administrativo para la consolidación de una estructura digital que sea capaz de abordar la ciberseguridad desde una dimensión proactiva a nivel legal y gubernamental, lo que de acuerdo con Ávila (2024), permite promover una cultura de seguridad compartida a nivel social por cuanto debe ser flexible y práctica para garantizar su aplicabilidad.

Esto debido a que uno de los puntos neurálgicos de ataque es la información en las instituciones públicas y consecuentemente hacia la administración público en su conjunto, por lo que las medidas de ciberseguridad no deben limitarse a la protección de datos sino al mantenimiento de los Estados sobre la base del principio de legalidad, transparencia y funcionalidad para lograr que se perpetúe la viabilidad de las instituciones estatales en el escenario digital (Ávila, 2024).

Así, la creciente digitalización de la mano con las estrategias de ciberseguridad obliga al desarrollo de ciudades inteligentes que sean capaces de integrar servicios e infraestructuras para la protección de la seguridad y privacidad como derechos tanto a escala individual como colectiva, de forma tal que se mitiguen los riesgos para garantizar la permanencia de los servicios esenciales desde una perspectiva de gestión de riesgos que no se limita a la tecnología sino también a otras prácticas y políticas públicas de planificación y colaboración multisectorial de protección de datos como es el caso de la Estrategia Nacional de Seguridad y Confianza Digital 2021-2026 que se encuentra siendo aplicada en países como Perú (Chalco *et al.,* 2024); lo que refuerza posturas de autores como Vera *et al.* (2022), para quienes la evaluación y categorización de los riesgos digitales debe integrar una serie de metodologías y estrategias ciudadanas de

control tanto formal como informal para que el ejercicio de los derechos inicie en la individualidad de los usuarios.

La era digital, por tanto, ha surgido de la mano con amenazas cibernéticas que se convierten en una responsabilidad directa del Estado no solo para la protección de sus estructuras sino de los ciudadanos con políticas y protocolos adecuados a la situación cibernética debido a la existencia de superficies de ataque ampliadas, datos convertidos en activos críticos, brechas legales y cadenas de suministro que se desenvuelven en un entorno cambiante de aprendizaje continuo y completamente interconectado (Cano y Monsalve, 2023). Lo que además según Kasper *et al.* (2021), se perfecciona con el establecimiento de una red de políticas interrelacionadas ciber-diplomacia que reflejan la unión de las políticas internas y externas incluyendo la prevención, reducción y salvaguarda de derechos (Safitra *et al.,* 2023).

Lo que permite determinar que los datos son el punto central de la necesidad regulatoria frente a la tecnología y la inteligencia artificial, convirtiéndose además en un medio conductor para la vulneración de otros derechos conexos e igualmente expuestos, exigiendo el establecimiento de lineamientos y protocolos que bajo ninguna circunstancia violen la privacidad especialmente en caso de información valiosa que, de no ser así, afectaría por completo la confianza de las personas en el Estado (González, 2023).

En este orden de ideas, Ecuador cuenta con un Acuerdo de Política de ciberseguridad N°006-2021 en el cual se expone que, “Ecuador entiende a la ciberseguridad como la capacidad del Estado para proteger a las personas, sus bienes activos de información y servicios esenciales ante riesgos y amenazas que se identifican en el ciberespacio” (p.9).

El texto, fundamenta que la ciberseguridad en Ecuador está intrínsecamente ligada a los deberes constitucionales del Estado, que incluyen la promoción y desarrollo de una cultura de paz, siendo que un entorno digital seguro constituye hoy en día un elemento de la estabilidad

social y económica; es así que el principio integral de la ciberseguridad implica que no solo se deben proteger los sistemas y datos informáticos, sino también impulsar un entorno digital seguro y confiable.

En este sentido, esta Política Nacional de Ciberseguridad (2021) abarca diversas competencias, como la ciberdefensa, que busca proteger la infraestructura crítica del país contra ataques cibernéticos; la ciber inteligencia, que se enfoca en anticipar y prevenir amenazas mediante la recolección y análisis de información digital; y la ciber diplomacia, que promueve la cooperación internacional para enfrentar amenazas cibernéticas transnacionales. De esta manera, el referido texto ejemplifica algunos de los ciberdelitos, tales como:

> La piratería, que afecta a la propiedad intelectual, los ataques con códigos maliciosos, como por ejemplo ataques de denegación de servicios, que constituyen amenazas a la seguridad de los gobiernos, negocios e individuos y que suponen un desafío para los organismos de seguridad y agencias encargadas de la aplicación de la ley, entre otros. (p.9)

Análisis de resultados y discusión

Hasta este punto de la investigación, se ha logrado determinar que la adopción de tecnologías emergentes ha generado mayor exposición de los datos personales e incrementado el riesgo de vulneración al derecho de privacidad, lo que se agrava con la limitada normativa vigente disponible para el abordaje de los retos actuales propios de la era digital y el ciber espacio, las nuevas tecnologías han alcanzado un nivel disruptivo frente a una tecnología estática y poco flexible, lo que se evidencia en la existencia de normativas que no se encuentran a la par del progreso tecnológico.

Es decir, existe en la actualidad una fuerte tensión entre el avance tecnológico y la garantía de derechos fundamentales, lo que conlleva a reafirmar el papel protagónico de la ciberseguridad en la protección del derecho a la privacidad y otros derechos conexos, lo que consecuentemente exige fortalecer la cohesión entre regulaciones jurídicas y estrategias

tecnológicas, - lo que Fraguas (2024) sostuvo sobre la imperiosa necesidad de medidas preventivas en el entorno digital-.

En este sentido, resulta imprescindible que se adopten estrategias de ciberseguridad como elemento integral en un marco normativo más allá de simples estrategias técnicas, de forma tal que sea posible alcanzar un equilibrio entre la innovación y la garantía de derechos fundamentales, lo que lleva a la proposición de principios éticos en el diseño y uso de tecnologías emergentes, garantizando un desarrollo tecnológico responsable, misma que deba enfocarse tanto en la prevención como la mitigación de riesgos sobre la base de principios éticos, bioéticos y morales que han dado forma a diversidad de mecanismos de protección de derechos, estos son:

Tabla 1 *Propuesta de principios éticos para el diseño y uso de tecnologías emergentes*

Propuesta de principios éticos para el diseño y uso de tecnologías emergentes	
Transparencia y aplicabilidad	Los sistemas deben ser comprensibles tanto para los usuarios como para los organismos de control, garantizando la existencia de decisiones auditables.
Consentimiento informado y autonomía.	La recopilación de datos debe ser capaz de respetar y garantizar el derecho a la autodeterminación informativa.
Seguridad.	Implica que las empresas desarrolladoras de tecnologías emergentes deben garantizar diseños robustecidos en términos de seguridad para la prevención de ciberataques, lo que va de la mano con el principio de responsabilidad y supervisión humana en virtud del cual los desarrolladores se vean en la obligación de rendir cuentas por el impacto de sus tecnologías.
Justicia y no discriminación.	Es imprescindible que las medidas de

	prevención y seguridad contemplen mecanismos orientados a evitar sesgos algorítmicos, de forma tal que se promueva el acceso y uso equitativo de la tecnología

Fuente: Elaboración propia

Conclusión

Con base a la información presentada en este artículo científico y, en atención a los objetivos planteados en la parte introductoria del mismo, se concluye que las nuevas tecnologías impactan considerablemente en el derecho a la privacidad por cuanto los datos se encuentran sobreexpuestos en las diversas redes interconectadas dentro del ciberespacio que plantea una nueva realidad alternativa, frente a lo cual es fundamental que se robustezcan las medidas y estrategias de ciberseguridad en forma de planes y políticas de protección de derechos.

En cuanto a los riesgos y desafíos para la privacidad derivados del uso de tecnologías emergentes, se colige que el Big Data y la gran disponibilidad de información incrementan los riesgos de ciberataques y amenazas digitales que vulneran derechos consecuentes a la privacidad y protección de datos, esto como consecuencia de la pérdida de la privacidad y la existencia de distintas plataformas que se nutren de información en el marco de una cuarta revolución industrial marcada por el progreso tecnológico.

En este sentido, la ciberseguridad desde el punto de vista jurídico en la protección de la privacidad tiene un rol preponderante en el marco tecnológico y social actual por cuanto implica la toma de decisiones técnicas fundamentadas en la necesidad de tutelar derechos fundamentales -tanto clásicos como emergentes- que se ven expuestos en la era digital, de ahí que bajo la necesidad de diseñar prácticas y políticas que permitan equilibrar la innovación tecnológica con el respeto a los derechos de los usuarios, se propuesto un conjunto de principios éticos para el

diseño y uso de tecnologías emergentes, entre los que se encuentra la transparencia y aplicabilidad, el consentimiento informado, la autonomía y la justicia.

Referencias

Agnese, C. (2016). Ciberseguridad: Un nuevo desafío para la comunidad internacional. Revista del Instituto Español de Estudios Estratégicos 1(1), 950-966. https://dialnet.unirioja.es/servlet/articulo?codigo=5998287

Asimbaya, A. (2024). La importancia de la ciberseguridad en las PYMES. Madrid: Universidad Rey Juan Carlos. https://burjcdigital.urjc.es/handle/10115/41040

Ávila, A. (2024). Seguridad de la información en instituciones públicas: desafíos y buenas prácticas en el contexto ecuatoriano. Journal of Economic and Social Science Research 4(2), 140-156. https://doi.org/10.55813/gaea/jessr/v4/n2/96

Beccerril, A. (2021). Retos para la regulación jurídica de la Inteligencia Artificial en el ámbito de la Ciberseguridad. Revista IUS 15(48), 9-34. https://www.scielo.org.mx/pdf/rius/v15n48/1870-2147-rius-15-48-9.pdf

Candau, J. (2021). Ciberseguridad. Evolución y tendencias. Revista del Instituto Español de Estudios Estratégicos 1(1), 460-494. https://dialnet.unirioja.es/servlet/articulo?codigo=8175398

Cano, J. (2022). Prospectiva de ciberseguridad nacional para Colombia a 2030. Revista Científica General José María Córdova 20(40), 815-832. http://www.scielo.org.co/pdf/recig/v20n40/2500-7645-recig-20-40-814.pdf

Cano, W. y Monsalve, S. (2023). Ciberseguridad, reto empresarial para afrontar la era de la digitalización actual. Universidad Pontificia Bolivariana. https://repository.upb.edu.co/bitstream/handle/20.500.11912/11318/Ciberseguridad%2C%

20reto%20empresarial%20para%20afrontar%20la%20era%20de%20la%20digitalización%20actual.pdf?sequence=1&isAllowed=y

Chalco, F.; Pérez, Y.; Quispe, J.; Flores, J.; Pari, Y.; Humpiri, J. y Mamani, E. (2024). Ciberseguridad en ciudades inteligentes: perspectivas legales sobre protección de datos y seguridad de infraestructuras en Perú. Tecnologia, Comunicação e Gestão da Inovação: contribuições para o desenvolvimento de novos conhecimentos 1(1), 61-73. https://downloads.editoracientifica.com.br/articles/240616933.pdf

Criado, M. (2021). La investigación en el mundo del derecho para la práctica judicial. En Lara, R. Manual de metodología para la investigación jurídica para la práctica judicial en la escuela judicial. Bogotá: Consejo Superior de la Judicatura, 23-60. https://escuelajudicial.ramajudicial.gov.co/sites/default/files/Manua%20Enero%202022.pdf

Dávalos, A. y Mujica, M. (2024). Ciberseguridad y vulneración de datos personales en entidades financieras, Lima 2022. Lima: Universidad Autónoma del Perú. https://repositorio.autonoma.edu.pe/bitstream/handle/20.500.13067/3512/Davalos%20Guillen%2C%20A.%20J.%2C%20%26%20Mujica%20Sanchez%2C%20M.%20L..pdf?sequence=1&isAllowed=y

Florabel, R. (2024). Los problemas ciber vistos desde el Derecho Internacional. Un gran reto a enfrentar. Eunomía. Revista en Cultura de la Legalidad 27(1), 155-182. https://doi.org/10.20318/eunomia.2024.9005

Flores de Valgaz, S.; Díaz, K. y Zambrano, G. (2024). El comercio electrónico y su incidencia en el derecho a la protección de datos personales. Portoviejo: Universidad San Gregorio de Portoviejo. http://repositorio.sangregorio.edu.ec/bitstream/123456789/3638/1/AC%20DÍAZ%20GA

NCHOZO%20KATHERIN%20YARITZA-ZAMBRANO%20GÉNESIS%20ANAHÍS%20ZAMBRANO.pdf

Fraguas, A. (2024). Derechos de privacidad en la era digital; retos y soluciones legales. Bezuz [en línea]. https://www.belzuz.net/es/publicaciones/en-espanol/item/11967-derechos-de-privacidad-en-la-era-digital-retos-y-soluciones-legales.html

Giant, N. (2016). Ciberseguridad para la i-generación: Usos y riesgos de las redes sociales y sus aplicaciones. Narcea Ediciones. https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://narcea ediciones.es/es/educacion-hoy/1108-ciberseguridad-para-la-i-generacion-9788427721432.html&ved=2ahUKEwiX3J3a4ImKAxX3gYQIHU6PAL4QFnoECEQQAQ&usg=AOvVaw33l2vYNzXrbUPKRsZ8egXL

González, L. (2023). Inteligencia artificial y derecho: retos jurídicos. Madrid: Comillas Universidad Pontificia. https://rep ositorio.comillas.edu /xmlui/bitstream/handle/11531/71410/TFG%20-%20Gonzalez%20Moreno,%20Laura.pdf?sequence=-1

González, M. (2015). España es, tras EEUU y Reino Unido, el país que sufre más ciberataques. España: El País. https://elpais.com/politica/2015/02/05/actualidad/1423136881_175042.html

Gutiérrez, C.; Carrillo, D.; Bermúdez, J.; Hidrogo, I.; Carrillo, R. y Sánchez, M. (2023). ChatGPT: oportunidades y riesgos en la asistencia, docencia e investigación médica. Gaceta Médica de México 159(1), 382-389. https://www.scielo.org.mx/pdf/gmm/v159n5/2696-1288-gmm-159-5-382.pdf

kasper, A.; Osula, A. y Molnár, A. (2021). EU cybersecuritu and cyber diplomacy. Dossier "Europe facing the digital challenge: obstacles and solutions 1(34), 1-15.

https://dialnet.unirioja.es/descarga/articulo/8398832.pdf

Leyva, A. (2021). Análisis de políticas públicas de seguridad cibernética. Estudio del caso ecuatoriano. Polo del Conocimiento, 6(3), 1229-1250. https://dialnet.unirioja.es/servlet/articulo?codigo=7926828

Martínez, I. (2023). Sobre los métodos de la investigación jurídica. Revista Chilena de Derecho y Ciencia Política 14(1), 1-4. https://doi.org/10.7770/rchdcp-V14N1-art312

Martínez, L. (2024). Virtualidad, ciberespacio y comunidades virtuales. Red Durango de Investigadores Educativos. http://www.upd.edu.mx/PDF/Libros/Ciberespacio.pdf

Mendivelso, J. (2024). Seguridad y Privacidad en el Tiempo Digital, la Era de la Información Liquida. Revista Multidisciplinar Ciencia Latina 8(2), https://doi.org/10.37811/cl_rcm.v8i2.11136

Miranda, R. (2023). La infancia y la adolescencia en la era digital: nuevos retos para la garantía de sus derechos. Revista Relacões Internacionais do Mundo Atual 4(42), 465-489. https://accedacris.ulpgc.es/bitstream/10553/127726/1/6449-371382766-1-PB.pdf

Montúfar, C. (2022). Marco regulatorio de la ciberseguridad y ciberdefensa dentro de la sociedad de la información y el conocimiento. Quito: Universidad Andina Simón Bolívar. https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://repositorio.uasb.edu.ec/handle/10644/9076&ved=2ahUKEwiDhrvh4ImKAxXpq4QIHVadD_kQFnoECBEQAQ&usg=AOvVaw0IZDt-O1HkiMQhYyw8j8dW

Plúas, A.; Muñozm D.; Moreira, O.; Cordovilla, J. y Cuenca, A. (2024). Sistema Jurídico Contemporáneo y el Derecho Administrativo en la Era de la Ciberseguridad. Polo del Conocimiento 9(11), 283-296. https://doi.org/10.23857/pc.v9i11.8277

Pons, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. Revista Latinoamericana de Estudios de Seguridad, (20), 80-93. https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://revista

s.flacsoandes.edu.ec/urvio/article/view/2563&ved=2ahUKEwiGuPXv4ImKAxWCSTABHd10GKIQFnoECAwQAQ&usg=AOvVaw12xoW701bHcmTa9TLhQX7I

Quispe. F. (2024). Los problemas cibervistos desde el Derecho Internacional. Un gran reto a enfrentar. Revista en Cultura de la Legalidad 1(27), 155-182. https://e-revistas.uc3m.es/index.php/EUNOM/article/view/9005/6753

Ramírez, A. (2021). Implementa la estrategia de análisis de contenido cualitativo con MAXQDA. MAXQDA [en línea]. https://www.maxqda.com/blogpost/analisis-contenido-cualitativo#:~:text=El%20análisis%20de%20contenido%20cualitativo%20es%20una%20estrategia%20o%20metodología,la%20agrupación%20de%20categorías%20temáticas.

Riofrío, J. (2012). Los delitos informáticos y su tipificación en la legislación ecuatoriana. Loja: Universidad Nacional de Loja. https://dspace.unl.edu.ec/jspui/handle/123456789/9329

Rivera, Y. y Maldonado, L. (2023). Vulneración del derecho a la privacidad dentro de la era digital en el Ecuador. Polo del Conocimiento 8(10), 982-1009. https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://dialnet.unirioja.es/descarga/articulo/9205974.pdf&ved=2ahUKEwidw6ukgsKLAxVsQjABHW2YNuMQFnoECBEQAQ&usg=AOvVaw1E9a4Cmnp8JkiEkKzZm-G8

Rodríguez, W.; Morales, L. y Cadavid, J. (2023). La construcción de la ciberseguridad en el Estado colombiano: un enfoque desde el derecho administrativo. Envigado: Institución Universitaria de Envigado. http://bibliotecadigital.iue.edu.co/bitstream/20.500.12717/3300/1/8.%20Articulo%20-%20La%20construcción%20de%20la%20Ciberseguridad%20en%20el%20estado%20Colombiano.pdf

Safitra, M.; Lubis, M.; y Fakhurroja, H. (2023). Counterattacking Cyber Threats: A Framework

for the Future of Cybersecurity. Sustainability 15(1), 1-32. https://doi.org/10.3390/su151813369

Santana, E. y Báez, K. (2022). Ciberespacio y Cibermundo: delimitaciones conceptuales desde el materialismo sistémico. Ciencia y Sociedad 47(1), 45-57. https://www.redalyc.org/journal/870/87070563004/html/

Solleiro, J.; Castañón, R.; Guillén, A.; Hernández, T. y Solís, N, (2022). Vigilancia tecnológica en ciberseguridad. El ABC de la Ciberseguridad. Boletín No. 1. https://www.icat.unam.mx/wp-content/uploads/2022/09/Vigilancia_Tecnologica_en_Ciberseguridad_Boletin.pdf

Subijana, I. (2008). El ciberterrorismo: Una perspectiva legal y judicial. Universidad del País Vazco. https://www.ehu.eus/documents/1736829/2176658/08+Subijana.indd.pdf

Vargas, R. y Herrera, L. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virual: modelo ecuatoriano de gobernanza en ciberdefensa. Revista Latinoamericana de Estudios de Seguridad. https://doi.org/10.17141/urvio.20.2017.2571

Vega, E.; Lemaitre, R.; Villegas, A. y Solís, C. (2024). Estado de la ciberseguridad en Costa Rica 2023. Nicoya: Universidad Nacional Costa Rica. https://repositorio.una.ac.cr/server/api/core/bitstreams/4902956c-5479-405f-b49b-64a0457964cf/content

Vera, M.; Navarro, G.; Gómez, J. (2022). Riesgos de la aceleración digital: una mirada desde el Marco DIGCOMP2.2 y los derechos digitales de la ciudadanía. Anuario ThinkEPI 16(1), 1-16. https://doi.org/10.3145/thinkepi.2022.e16a19